Controls Worksheet

# Purpose

The purpose of this worksheet is to document implemented security controls associated with an asset or a group of assets. Refer to the [Information Security Guideline](http://ciso.washington.edu/site/files/Information_Security_Guideline.pdf) for more details on the controls outlined in [Administrative Policy Statement 2.6](http://www.washington.edu/admin/rules/policies/APS/02.06.html).

NOTE: When filled out, this document or information therein is classified as Restricted and may be exempted from a public records request on the basis of security; pursuant to RCW 42.56.420.

# Audience

Service support teams use this worksheet to document security controls for an asset or a group of assets. Service clients, service managers, and service owners use this document to assess security characteristics of the service.

# How To Use This Worksheet

* Controls are broken down into six categories that align with APS 2.6. There is a table for each category.
* Describe how you have implemented the control in the 'Description' column. Example text is in blue.
* List supporting tools or services maintained by other organizations in the ‘Resources' column.
* If you have any assumptions, list them.
* If existing documentation addresses a control (even in part), then reference it.
* There is no need to create documentation if it does not already exist - mark it as a gap.
* Refer to the [Information Security Guideline](https://ciso.uw.edu/site/files/Information_Security_Guideline.pdf) for more details on controls and examples.

|  |
| --- |
| **Asset Information** |
| **Asset description and function**Provide a brief overview of the asset (or asset group). What is it? What does it do? Who are the customers? |  |
| **Link to associated security plan**This worksheet is meant to be focused on a particular asset or group of assets and supplemental to an organization’s security plan. |  |
| **Asset architecture**Import or link to a system architecture diagram that assists interpretation of the security of this asset. Diagram should reflect relationships between the asset and its dependencies. Helpful features include servers, server names, links to dependencies, apps, databases, other software servers, interfaces. |  |
| **Data classification and volume**Provide a brief overview of the data stored, processed, or transmitted by the asset.[See: Data Classifica](https://privacy.uw.edu/policies/data-classifications/)tions |  |
| **Asset Location**Where is the asset located - on premise (which data center), in the cloud (which vendor), or hybrid? |  |
| **Asset Owner** |  |
| **Asset Manager** |  |
| **Author** |  |
| **Last Review** |  |
| **Last Update** |  |

|  |  |  |
| --- | --- | --- |
| **Control** | **Description** | **Resources** |
| General Operational Controls |  |  |
| **A change and configuration management process**Describe your practices for documenting, reviewing, and approving changes to the baseline configuration of assets. Include roles and responsibilities. Include a list of individuals/groups that would need to be notified of a change. Include any practices for reversing or removing changes that cause problems. | Our staff follow an established and documented internal <<Change Management Process>> for proposed changes made to our managed production systems. The process includes review and analysis to identify potential security and service-related impacts prior to implementation. Approved changes are validated on test systems when possible before deploying to production systems. Stakeholders are notified before changes are made to production systems. Systems are monitored after changes are implemented to ensure expected results and changes are rolled back if necessary.We maintain a record of technical configurations for our managed systems. This allows for identifying unexpected or unplanned changes to production systems and to rebuild or restore a system to an approved state if necessary. | [Ymir](https://barista.cac.washington.edu/ymir/view/%22%20/) Configuration Item Management Tool[Jira](https://jira.cac.washington.edu/projects/SISPROD/summary) Project Management system[UW IT Connect](https://itconnect.uw.edu/work/administrative-systems/uw-connect/) service management platform |
| **A flaw remediation process**Describe your practices for identifying, reporting, assessing, prioritizing, and correcting potential vulnerabilities. Be sure to describe how the remediation process works in conjunction with the change management process. Include roles and responsibilities, targets for the resolution of problems, expected response times, and a definition of ‘response’. List any individuals or groups that would need to be included in problem resolution (e.g., groups or tags that need to be added to a trouble ticket). | As a regular operational activity, functional patches are evaluated and reviewed by staff before they are deployed following the Change Management Process outlined above. For all updates, change monitoring systems verify and validate the application of updates to systems. This automated process is further supported by business procedures intended to inform relevant personnel of changes.  | Multiple sources are used in an effort to obtain current information about required security patches, especially on applications:* Vendor product support channels
* UW Office of the CISO weekly Cyber Intelligence Report
* [SCCM](https://itconnect.uw.edu/wares/uware/microsoft/ms-server-software/) for finding and updating 3rd party software
* [WSUS](https://itconnect.uw.edu/wares/uware/microsoft/ms-server-software/) - find and updating OS related software for Servers or workstations
* Windows Update for Business (UW-IT) only for Windows 10 Enterprise
 |
| **A malicious code and unauthorized software countermeasure process**Describe the antivirus and antimalware solutions that you have implemented. Describe your process for keeping these solutions up to date. If you have identified authorized software, describe how you detect and address unauthorized software. | Sophos anti-virus software is installed on systems as appropriate and is configured to automatically remediate identified threats, and to automatically check for and install updates and new definition files.Operating systems are configured to automatically download and install security patches or are patched manually as security updates become available.  | The McAfee Intrusion Prevention System (IPS), managed by the Office of the CISO, is used to monitor network traffic to detect and prevent malicious threats.[Sophos anti-virus](https://itconnect.uw.edu/wares/uware/sophos-anti-virus-software/) Office 365 is configured to automatically scan email attachments for malicious code. |
| **A data protection and destruction process**Describe your practices for handling UW Confidential or Restricted data and the media or devices that store it. Describe your practices for securely transporting those media and devices outside of designated areas. Describe your practices to protect against the unintended exposure of UW Confidential or Restricted information when the information is no longer needed (e.g., pulverize, shred, burn, or electronically overwrite the data prior to disposal.) | Data Protection controls:* Limiting access to data to only authorized personnel using the principle of least privilege
* The use of security groups to manage user access to systems and data
* Requiring unique assigned UW NetIDs and two-factor authentication to connect to systems
* Network Segmentation
* Encrypting data in transit and encrypting data at rest where possible and appropriate
* Using LastPass password manager to securely store system and administrator account information
* Configuring our systems using industry established best practices, including but not limited to, The Center for Internet Security (CIS) Benchmarks
* Utilizing a private subnet for departmental resources that is behind a managed firewall
* Requiring the use of a UW-IT managed VPN to remotely connect to departmental resources from IP addresses outside of the private subnet

Data Destruction controls: Devices that store data are securely decommissioned or destroyed by UW Surplus Disposal following [federal government standards](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf) to ensure data is not recoverable.We adhere to UW Data Governance standards and UW records management and file retention policies as well as to our own <<Departmental Records Retention Schedule>>. | [UW Surplus](https://facilities.uw.edu/catalog/surplus)[UW Records Management Services](https://finance.uw.edu/recmgt/)[UW Data Governance](https://www.washington.edu/data-governance/)[CISO Office](https://ciso.uw.edu/2018/11/16/bitlocker-ineffective-on-self-encrypting-drives/#gpo) about Windows BitlockerMac filevault [by Apple](https://support.apple.com/en-us/HT204837)[HuskyOnNet VPN](https://itconnect.uw.edu/connect/uw-networks/about-husky-onnet/use-husky-onnet/) |
| **Secure development practices**Describe your application/system/software development lifecycle practices. Describe your secure coding practices. Describe how you handle production and test data and how you manage your test and development environments. Describe what security testing you do to identify potential vulnerabilities. Describe what practices you use when contracting with a third-party developer. | An agile SDLC methodology is used by the development team. The use of this methodology has resulted in strong controls over capturing business requirements, source code version management, cross-discipline quality assurance testing. Some of the <<Development Practices>> include:* Source code repositories with access controlled by UW Groups service
* Secrets (passwords, keys) are not stored in source
* Code is peer reviewed
* Automated tools are used to meet development standards
* Deployed code is regularly validated, and any variance is eliminated and reported
 | Development tools include [GitHub](https://uw.service-now.com/sp?id=sc_entry&sys_id=9fb5de4e13777f0811cdd2f18144b01f&sysparm_category=dd1970e1dba6bf40d6a77a8eaf961946) and Bitbucket.[DevOps](https://dev.azure.com) -(previously [Visual Studio Code](https://itconnect.uw.edu/wares/uware/visual-studio-annual-subscription/)) |
| **Backup and recovery processes for critical information and software**Describe how you determine backup needs and requirements. Include how and when backups are conducted, how backups are protected, and under what conditions backups are tested. | Most data backups are stored on an encrypted hard drive. For those backup drives which are not able to feasibly encrypt, the compensating control is to locate the backup drive within a physically secure data center with highly restricted access to only a limited number of key personnel. All backup tapes are encrypted.Automated backups of key systems are made to UW-ITs TSM (Tivoli Storage Manager) backup service. Backups are encrypted using (AES) 256-bit encryption. Encryption keys are managed within UW-IT by personnel with root privileges and are not accessible by anyone else. We maintain a list of all systems backed up to UW-IT TSM in [Ymir](https://barista.cac.washington.edu/ymir/view/%22%20/). | [Data Backup service](https://uw.service-now.com/sp?id=sc_entry&sys_id=8041d325db12fb8037ae9ec6db96194a&sysparm_category=5942fc69db62bf40d6a77a8eaf96190b)[UW-IT AutoPilot](https://itconnect.uw.edu/wares/msinf/aad/device/intune/autopilot/) to recover Windows to initial install |
| **A business continuity and disaster recovery plan**Describe how you have identified your business continuity and disaster recovery requirements, what plans you have in place, and under what conditions these plans are rehearsed. | Business continuity and disaster recovery (BC/DR) practices apply to all critical assets, each with their own Recovery Time Objective (RTO) and Recovery Point Objective (RPO). DR plans are managed <<here>>.Additional safeguards are in place that would allow for BC/DR options under certain conditions, including: * Ability for all staff to work remotely
* Multiple ways for staff to contact and collaborate with each other (Email, Slack, MS Teams, Zoom, phone).
 | [UW-IT Disaster Recovery Documentation](https://wiki.cac.washington.edu/display/TBC/UW-IT%2BDisaster%2BRecovery%2BDocumentation)  [UW-IT Geographic Redundancy Failure Scenarios and Recovery Strategies](https://wiki.cac.washington.edu/display/TBC/UW-IT%2BGR%2BFailure%2BScenarios%2Band%2BRecovery%2BStrategies)[HuskyReady](https://uw.kuali.co/ready/users/sign_in) for backup DR/BC Plans |
| **Information security technical architecture standards**Describe your practices for design, development, and engineering that promote security. | The general approach to designing and implementing pragmatic solutions has been to give priority to addressing actual risks, to favor stronger controls, and to treat security as a core value. Some areas of focus include: * Input validations on front end
* API parameter validations and controls
* Access logging and cross component tracing
* Authenticated and authorized access of specific controls and features.
* Isolation and separation of production environment from dev/test
 | [MSFT Viso](https://itconnect.uw.edu/connect/productivity-platforms/microsoft-productivity-platform/visio/) (UW-IT) for creating diagram of data flows and business processes. |
| **System build and maintenance standards**Describe your baseline configurations for hardware, authorized software, and systems. Describe your procurement, installation and maintenance processes and procedures. | Server builds, baseline configurations, and maintenance procedures for departmental managed systems are documented in the <<wiki>>.Workstation builds follow an established standard build <<checklist>>.Maintenance: System administrators perform sysadmin duties from clean, dedicated workstations, or VMs running on an equally dedicated workstation. | [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/) (sign up with UW email)[IT Sourcing](https://itconnect.uw.edu/work/it-sourcing/)[UW Procurement forms](https://finance.uw.edu/ps/suppliers/terms-conditions) |
| **Acceptable use standards**Describe your process to inform workforce members of their responsibilities related to information, infrastructure technology, and information systems. | Staff are made aware that their use of UW systems may be monitored, recorded and subject to audit. Unauthorized use of any University system is prohibited, and such use may be subject to criminal and civil penalties. Use of a University system indicates consent to monitoring and recording.UW-IT staff must read and accept the [Access and Use Agreement](https://uwnetid.washington.edu/agree/). Managers can run a report to check to see if staff have done so.Student staff are required to sign a <<Non-Disclosure Agreement>> in addition to the Access and Use Agreement. | [Access and Use Agreement](https://uwnetid.washington.edu/agree/).[Access and Use Agreement - Report](https://www.washington.edu/intech/hr/people/idaa/) |

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Description** | **External Resources** |
| Technical Security and Access Controls |  |  |
| **Remote access process**Describe how you manage access to your assets from locations not under the University’s control. | Remote connection to the departmental private network requires using Husky OnNet-Department (HON-D) VPN. Access is limited only to authorized staff via security group membership. | [Husky OnNet](https://itconnect.uw.edu/connect/uw-networks/about-husky-onnet/) |
| **Cryptographic controls for protecting data**Describe what cryptographic methods (e.g., electronic signatures, encryption) you use to reduce the likelihood that institutional information is read, modified, or otherwise utilized by an unauthorized individual. | All departmental laptops are encrypted using Microsoft BitLocker or Apple FileVault. Backups of departmental systems are encrypted using (AES) 256-bit encryption. Connections to departmental systems from external IPs require the use of HON-D VPN, encryption keys and certificates.For applications that handle sensitive data, TLS is used to encrypt data in transit. | [CISO Office](https://ciso.uw.edu/2018/11/16/bitlocker-ineffective-on-self-encrypting-drives/#gpo) about Windows BitlockerMac filevault [by Apple](https://support.apple.com/en-us/HT204837) |
| **An access authorization process for all users and information systems**Describe how you manage who or what has access to your assets as well as the type of access that you permit. | Each employee is issued a unique UWNetID that is used to log on to departmental systems. Applications that need access to other applications or databases have their own unique accounts.Permissions to resources and systems are assigned following the principle of least privilege and the principle of least functionality. Administrators have separate accounts - a user account, and an administrative account.Requests for access are made using UW-IT's service management platform and are logged for periodic auditing. Account access and associated privileges is reviewed regularly to determine if they are still valid. | [ASTRA Access Management](https://uw.service-now.com/sp?id=sc_entry&sys_id=2dc2d1d9db9a7308d6a77a8eaf961964) [UW Groups Service](https://groups.uw.edu/)[Manage UW Resources](https://uwnetid.washington.edu/manage/) |
| **An authentication mechanism for all authorized users and information systems**Describe what authentication mechanisms (e.g., account lockout, password length and complexity, two-factor token-based authentication, restrict access to privileged functions) you use to validate the identity of a workforce member, service, or information system when they use one of your assets. | UW-IT’s SAML-based UWNetID identity management infrastructure is leveraged to provide authentication. Based upon sensitivity, systems use Duo two-factor authentication. | [Single sign-on with UW NetID](https://itconnect.uw.edu/security/iam/sso/) [Duo 2FA](https://itconnect.uw.edu//security/uw-netids/2fa/)[Active Directory authentication](https://itconnect.uw.edu/wares/msinf/)[NETID - Delegated OU](https://itconnect.uw.edu/wares/msinf/ous/) admins[Kerberos](https://wiki.cac.washington.edu/x/dRcrAQ) |
| **Network, system, and application level protection measures**Describe how you have implemented appropriate security boundaries and layers of controls. Describe how you have separated user and system management functionality. Describe how you manage data sharing. | We have a designated private subnet. We subscribe to the UW-IT Managed Firewall service. Firewall rules only allow those ports and protocols with a <<documented>> business need; all other ports and protocols are blocked by default.Local firewalls are enabled on departmental workstations and servers.To ensure event data can be correlated, all critical assets maintain time synchronization with the UW NTP servers. | [Private Address Routing](https://itconnect.uw.edu/connect/uw-networks/network-addresses/private-address-routing/) UW-IT [Managed Firewall Service](https://itconnect.uw.edu/connect/uw-networks/firewall/) |

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Description** | **External Resources** |
| Monitoring Controls |  |  |
| **A baseline measurement process for application, system, and network activity**Describe how you create and maintain baseline measurements of normal activity. | Flower monitor is used to perform daily netflow queries and sends notifications for any unexpected network flows.Hoover: Zabbix server that provides monitoring metrics that include network utilization, CPU load and disk space consumption for various managed systems.Open Source HIDS Security (OSSEC) is used to monitor departmental hosts and performs log analysis, integrity checking, Windows registry monitoring, rootkit detection and notifies of anomalies, unexpected changes, and potential malicious activity. |  |
| **A monitoring capability for critical systems**Describe how you monitor your assets to detect and assess activity that varies from baseline measurements. | Both application and OS-level activity are monitored for departmental managed systems. These systems are supported with documented procedures. Amongst the controls are objects to detect events which may indicate unauthorized changes. A Zabbix server provides monitoring metrics that include network utilization, CPU load and disk space consumption for various managed systems. | The Office of the CISO maintains and regularly monitors a McAfee Intrusion Prevention System.The Office of the CISO monitors unauthorized use of UW NetID administrator credentials.[MSFT CloudAppSecurity](https://uwnetid.portal.cloudappsecurity.com/) (UW-IT Contract)  |
| **An intrusion detection mechanism**Describe how you detect, assess, and alert on attacks. | Host-based intrusion detection system (HIDS) is a component of the infrastructure assets. Our HIDS is used to detect unauthorized changes, attack signatures, and correlated events which may require further attention. | The Office of the CISO maintains and regularly monitors a McAfee Intrusion Prevention System.The Office of the CISO monitors unauthorized use of UW NetID administrator credentials.[Wazuh (UW MSFT Teams Video/presentation](https://web.microsoftstream.com/video/51ceb6fb-abb1-4c7a-a1cc-cbc76c25e464)) |
| **Logging processes for networks, systems, and applications**Describe how you are capturing information associated with network, system, and application activities to detect anomalies, address operational issues, and support incident response processes. Include how you synchronize systems clocks, protect logs, review logs, and act on logged information. | We capture system and user activities via a combination of standardized mechanisms (e.g. Apache web logs), centralized repositories (e.g. Splunk), and application-specific logging processes which store logs on the systems where the transactions and activities took place. Logs are regularly reviewed and events, alerts, advisories, anomalies, etc. are assessed and addressed. Logs are kept for 90 days. Access to all log data is highly restricted both with respect to whom and how they can be read and written to. | The Office of the CISO maintains a system of computers that provide log collection and analysis for the UW.[CISO Logging Cheat Sheet reference](https://ciso.uw.edu/2018/10/15/logging-cheat-sheets/)[Sysmon for Windows](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon) Logging on a Budget. Windows ATP for those whom have money |

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Description** | **External Resources** |
| Physical Controls |  |  |
| **Physical protection and access processes for buildings that house critical information technology and systems**Describe how you protect the facilities that house your assets from physical and environmental harm (e.g., locked doors, access card reader, and Uninterruptible Power Supply, water and smoke sensors). Describe how you limit access to designated areas to authorized individuals, detect unauthorized access, and deal with visitors. | Systems that store sensitive information are located in UW-IT managed data centers that utilize security guards, physical locks or electronic key card (plus PIN) access to limit access to only authorized personnel. Keys and key cards are assigned only to authorized individuals. Access is audited regularly and removed when no longer needed.  | [Data Center Co-Location service](https://uw.service-now.com/sp?id=sc_entry&sys_id=88cd79cddb9f3bc437ae9ec6db961961)[Campus Automated Access Management System](https://facilities.uw.edu/catalog/keys-and-building-access) (CAAMS)[UW Housing Desk Services](https://hfs.uw.edu/Contact-Us)[UW Building Coordinators](https://facilities.uw.edu/bldgcoord)[UW Lock Shop](https://facilities.uw.edu/contact) |
| **A physical protection process for critical information systems and institutional information**Describe your practices to safely store and reasonably protect media and devices containing University Data from physical compromise, theft, or destruction (e.g., stored in a locked container or room). | Systems that store sensitive information are located in designated rooms or data centers that utilize physical locks or electronic key card access to limit access to only authorized personnel. Keys and key cards are assigned only to authorized individuals. Access is audited regularly and removed when no longer needed.Entry into the departmental office suite requires key card access. Only authorized staff have access. Access is granted and removed as part of the on and off-boarding processes. | [Data Center Co-Location service](https://uw.service-now.com/sp?id=sc_entry&sys_id=88cd79cddb9f3bc437ae9ec6db961961)[Campus Automated Access Management System](https://facilities.uw.edu/catalog/keys-and-building-access) (CAAMS)[UW Housing Desk Services](https://hfs.uw.edu/Contact-Us)[UW Building Coordinators](https://facilities.uw.edu/bldgcoord)[UW Lock Shop](https://facilities.uw.edu/contact) |

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Description** | **External Resources** |
| Asset Identification Controls |  |  |
| **A process to identify, inventory, assign accountability, and classify institutional information and information systems**Describe how you identify and classify what data is stored, processed, or transmitted by your assets. | Departmental information assets are identified and aligned with Services described in the Organization section of the Departmental security plan. Data is classified according to UW data classification guidelines. | [Data Classifications](https://privacy.uw.edu/design/data-classifications/)Configuration item management service, [Ymir](https://barista.cac.washington.edu/ymir/view/).[Technology Dependency Analysis Tool (TDAT)](https://barista.cac.washington.edu/tdat/) used to define and manage the relationships between configuration items to determine the geographic resiliency of critical systems.[Equipment Database for UW Information Technology](https://barista.cac.washington.edu/edb/)If you connect to an Active Directory, a domain admin can find all systems that connect to it.[MSFT Compliance Center](https://compliance.microsoft.com/homepage) (UW-IT Contract) will allow policies to label classifications |

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Description** | **External Resources** |
| Account and Identity Management Controls |  |  |
| **An identity and eligibility verification and registration process**Describe your process to ensure workforce members are who or what they say they are, and that access is uniquely and appropriately assigned based on job duties or functions. | New employees must pass both satisfactory reference checks and a third-party background check before they are eligible for employment.UW-IT’s Identity Registration service is used to establish identity credentials. | [Identity Registration Service](https://uw.service-now.com/sp?id=sc_entry&sys_id=48c1901bdb8377c037ae9ec6db9619e8&sysparm_category=aca5b865db26bf40d6a77a8eaf96198b) |
|  **A user and system account life cycle management process**Describe your user and system account life cycle management process. Include defined account types (e.g., individual, group/shared, system, application, guest/anonymous, and temporary), expectations and limitations for account use, and the processes for creating, activating, modifying, disabling, and removing accounts. | We require that all supported systems and applications define their account types, levels of access for each account type, and who/who should not be granted access, documented <<here>>.We follow a staff provisioning and de-provisioning checklist: <<Staff Access Provisioning List>> to ensure that employees 1) are only granted individual or group/shared access to systems that they are authorized to have access to, and 2) will lose access to these systems when they are no longer employees.  | [UWNetID management services](https://uw.service-now.com/sp?id=sc_entry&sys_id=6585dd99db1e7308d6a77a8eaf9619fc&sysparm_category=aca5b865db26bf40d6a77a8eaf96198b) [UW-IT New Employee Checklist](https://wiki.cac.washington.edu/display/supvtools/Checklist%2Bfor%2Bnew%2Bemployees)[UW-IT Separating Employee Checklist](https://wiki.cac.washington.edu/display/supvtools/Checklist%2Bfor%2Bseparating%2Bemployees) |